MATHÉMATIQUES - SPÉCIALITÉ

F.HUMBERT

Table des matières

Chapitre A - Congruences 2

Chapitre B - PGCD 5

Chapitre C - Nombres premiers 11

Chapitre D - Matrices et évolution de processus 14

Chapitre E - Matrices carrées inversibles 17

Chapitre F - Matrices et études asymptotiques 20

Chapitre A - Congruences

1. Divisibilité

1.1. Cours.

Définition 1. Pour tous entiers relatifs m et n, m **divise** n ssi il existe un entier relatif k tel que $n = km$.

Notation 1. On note $m|n$.

Remarque 1. Tout entier relatif est un diviseur de 0.

Théorème 1. $\forall p, q, r \in \mathbb{Z}, \begin{cases} p|q \\ q|r \end{cases} \Rightarrow p|r$

Théorème 2. *Si p divise m et n alors p divise toute combinaison linéaire à coefficients entiers de m et n.*

2. Division euclidienne

2.1. Cours.

Axiome 1. *Tout ensemble non vide d'entiers naturels admet un plus petit élément.*

Théorème 3. $\forall n \in \mathbb{Z}, \forall m \in \mathbb{N}^*, \exists! q \in \mathbb{Z}, \exists! r \in \mathbb{N}, \begin{cases} n = mq + r \\ 0 \leq r < m \end{cases}$

q est le quotient et r le reste de cette ***division euclidienne****.*

Exemple 1. $328 = 17 \times 19 + 5$, $q = 19$, $r = 5$

Exemple 2. $-328 = 17 \times (-20) + 12$, $q = -20$, $r = 12$

Démonstration. Soit $E = \{k \in \mathbb{N} / km > n\}$.

Existence lorsque n>0

$\begin{cases} m \geq 1 \\ n + 1 > n \end{cases}$ donc $(n+1)m > n$ donc $n + 1 \in E$ donc $E \neq \{\}$ donc E admet un plus petit élément k_0.

Soit $q = k_0 - 1$ et $r = n - qm$.

$qm + r = n$

$(k_0 - 1)m \leq n < k_0 m$ donc $0 \leq n - (k_0 - 1)m < m$ donc $0 \leq n - qm < m$ donc $0 \leq r < m$.

Existence lorsque n<0

On se ramène au cas précédent en effectuant la division euclidienne de $-n$ par m : $-n = qm + r$ et $0 \leq r < m$.

$n = -mq - r = (-q - 1)m + (m - r)$

Si $r = 0$, la première expression est la division euclidienne cherchée, sinon c'est la deuxième. Dans ce dernier cas, on vérifie la condition sur le reste :

$0 < r < m$ donc $-m < -r < 0$ donc $0 \leq m - r < m$

Existence lorsque n=0

$n = m \times 0 + 0$ et $0 \leq 0 < m$

Unicité

Supposons qu'il existe deux divisions euclidiennes différentes : $n = m \times q + r = m \times q' + r'$.

$(q - q')m = r' - r$

$\begin{cases} 0 \leq r < m \\ 0 \leq r' < m \end{cases}$ donc $-m < r' - r < m$ or $r' - r$ est divisible par m donc $r' - r = 0$ or (1) donc $q - q' = 0$.

Absurde ! □

Remarque 2. Plus de dénominateurs en Spécialité.

2.2. **Travailler son cours.**

Exercice 1. On note q et r le quotient et le reste de la division euclidienne de a par b. Vrai/Faux

(1) Le reste de la division euclidienne de 2a par b est 2r.
(2) Le quotient de la division euclidienne de 2a par b est 2q.
(3) Le reste de la division euclidienne de a par q est r.
(4) Le reste de la division euclidienne de -a par b est b-r.

3. Congruences

3.1. **Cours.**

Définition 2. Soit $n \in \mathbb{N}^*$. Soit $a, b \in \mathbb{Z}$. a et b sont **congruents** modulo n ssi $a - b$ est divisible par n.

Notation 2. Elles sont nombreuses ! $a \equiv b\ [n]$, $a \equiv b\ mod\ n$, $a = b\ [n]$, $a = b\ mod\ n$

Théorème 4. *Pour tous entiers relatifs a et b et tout entier naturel n non nul :*
$a \equiv b\ [n]$ ssi a et b ont même reste pour la division euclidienne par n.

Démonstration. Soit les divisions euclidiennes de a et b par n : $a = nq + r$ et $b = nq' + r'$.
$a - b = n(q - q') + r - r'$
$\begin{cases} 0 \leq r < n \\ 0 \leq r' < n \end{cases}$ donc $-n < r - r' < n$
Supposons que $a \equiv b\ [n]$.
$a \equiv b\ [n]$ donc $a - b$ est divisible par n or $r - r' = (a - b) - n(q - q')$ donc $r - r'$ est divisible par n or $-n < r - r' < n$ donc $r - r' = 0$
Réciproquement, supposons que $r = r'$.
$a - b = n(q - q')$ donc $n | a - b$ donc $a \equiv b\ [n]$. □

Théorème 5. *Soit $n \in \mathbb{N}^*$, $k \in \mathbb{N}$. Soit $a, a', r, r' \in \mathbb{Z}$ tels que* $\begin{cases} a \equiv r\ [n] \\ a' \equiv r'\ [n] \end{cases}$.

(1) $a + a' \equiv r + r'\ [n]$
(2) $a - a' \equiv r - r'\ [n]$
(3) $a \times a' \equiv r \times r'\ [n]$
(4) $a^k \equiv r^k\ [n]$

Remarque 3. ATTENTION $k \equiv k'\ [n]$ n'implique pas $a^k \equiv a^{k'}\ [n]$. Contre-exemple $a = 2$, $n = 3$, $k = 1$, $k' = 4$.

Remarque 4. Désormais on traduira tout en termes de congruence (divisibilité, division euclidienne) et on appliquera le théorème précédent en le mimant correctement.

Exemple 3. Déterminer le reste de la division euclidienne de 25×2^n par 7.

3.2. **Travailler son cours.**

Exercice 2. Les mains dans le dos.

(1) Un billet de 10 € a pour numéro U09884536547. En remplaçant la lettre par son rang dans l'alphabet, on obtient un nombre à 12 ou 13 chiffres. ce nombre doit avoir 8 comme reste de la division euclidienne par 9. Peut-on affirmer que c'est un faux !

(2) Vérifier qu'un de vos billets n'est pas un faux.

(3) Déterminer le chiffre manquant d'un billet non falsifié de numéro U49834 ?82406.

Chapitre B - PGCD

1. PGCD

1.1. Cours.

Définition 3. Soit $(a;b) \neq (0;0)$ un couple d'entiers naturels. $pgcd(a;b)$ est le **plus grand diviseur commun** de a et b.

Dans la suite de ce chapitre, on note $D(a)$ l'ensemble des diviseurs strictement positifs de a et $D(a;b)$ l'ensemble des diviseurs strictement positifs de a et b. Cette notation n'est pas universelle et doit être redéfinie si elle est utilisée dans une copie.

Théorème 6. *Soit $(a;b) \neq (0;0)$ un couple d'entiers naturels.*

(1) $pgcd(a;b) = pgcd(b;a)$
(2) $pgcd(a;0) = a$
(3) $b|a \Rightarrow pgcd(a;b) = b$

Démonstration. □

(1) $\forall x \in D(a;b)$, $x \leq max(a;b)$ donc $D(a;b)$ est fini or $1 \in D(a;b)$ donc $D(a;b)$ est fini et non vide donc $D(a;b)$ possède un plus grand élément qui est $pgcd(a;b)$ or $D(a;b) = D(a) \cap D(b) = D(b) \cap D(a) = D(b;a)$ donc $pgcd(a;b) = pgcd(b;a)$.
(2) $D(0) = \mathbb{N}^*$ donc $D(a;0) = D(a) \cap D(0) = D(a) \cap \mathbb{N}^* = D(a)$ donc $pgcd(a;0) = a$
(3) $b|a \Rightarrow D(b) \subset D(a) \Rightarrow D(a;b) = D(a) \cap D(b) = D(b) \Rightarrow pgcd(a;b) = b$

Lemme 1. *Soit $a, b \in \mathbb{N}^*$. Soit r le reste de la division euclidienne de a par b. $pgcd(a;b) = pgcd(b;r)$.*

Démonstration. Soit $a = bq + r$ la division euclidienne de a par b.

Montrons que $D(b;r) \subset D(a;b)$.

Soit $d \in D(b;r)$. $d \in D(b;r)$ et $a = bq + r$ donc $d \in D(a)$

$d \in D(b;r)$ donc $d \in D(b)$

$\begin{cases} d \in D(a) \\ d \in D(b) \end{cases}$ donc $d \in D(a) \cap D(b)$ donc $d \in D(a;b)$.

Montrons que $D(a;b) \subset D(b;r)$.

Soit $d \in D(a;b)$. $d \in D(a;b))$ et $r = a - bq$ donc $d \in D(r)$

$d \in D(a;b)$ donc $d \in D(b)$

$\begin{cases} d \in D(b) \\ d \in D(r) \end{cases}$ donc $d \in D(b) \cap D(r)$ donc $d \in D(b;r)$.

On a montré que $D(a;b) = D(b;r)$ donc $pgcd(a;b) = pgcd(b;r)$. □

Exemple 4. Déterminer le pgcd de 364 et 247 en utilisant l'**algorithme d'Euclide**.

Théorème 7. *Cet algorithme s'arrête toujours et produit bien ce qu'il prétend.*

Démonstration. sur un exemple □

Théorème 8. *Les diviseurs communs de a et b sont les diviseurs de $pgcd(a;b)$.*

Démonstration. D'après la démonstration précédent, $D(a;b)$ est égal à l'ensemble des diviseurs du dernier reste non nul dans l'algorithme d'Eulide, c.a.d. à l'ensemble des diviseurs de $pgcd(a;b)$. □

Théorème 9. *Soit $(a;b) \neq (0;0)$ un couple d'entiers naturels. Soit $k \in \mathbb{N}^*$. $pgcd(ka;kb) = k \times pgcd(a;b)$.*

Démonstration. sur un exemple. On réécrit l'algorithme d'Euclide en multipliant tout par k. □

2. Théorème de Bézout

2.1. Cours.

Définition 4. Deux entiers naturels non nuls a et b sont **premiers entre eux** ssi $pgcd(a;b) = 1$.

Théorème 10. *$\frac{a}{pgcd(a;b)}$ et $\frac{b}{pgcd(a;b)}$ sont premiers entre eux.*

Démonstration. $pgcd(a;b) = pgcd(pgcd(a;b)\frac{a}{pgcd(a;b)}; pgcd(a;b)\frac{b}{pgcd(a;b)}) = pgcd(a;b) \times pgcd(\frac{a}{pgcd(a;b)}; \frac{b}{pgcd(a;b)})$
or $pgcd(a;b) \neq 0$ donc $pgcd(\frac{a}{pgcd(a;b)}; \frac{b}{pgcd(a;b)}) = 1$ □

Théorème 11. ***Identité de Bézout*** $\forall a, b \in \mathbb{N}^*$, $\exists u, v \in \mathbb{Z}$, $ua + vb = pgcd(a;b)$.

Démonstration. Soit $E = \{ma + nb \in \mathbb{N}^* / m, n \in \mathbb{Z}\}$. $a \in E$ donc $E \neq \{\}$ donc E contient un plus petit élement qu'on appelle d donc $\exists u, b \in \mathbb{Z}, d = ua + vb$.

Montrons que $pgcd(a;b) \leq d$.

$pgcd(a;b)$ divise toute combinaison linéaire de a et b donc il divise d donc $pgcd(a;b) \leq d$.

Montrons que $d \leq pgcd(a;b)$

Soit $a = dq + r$ la division euclidienne de a par d. $r < d$

$r = a - dq = a - (ua + vb)q = a(1 - uq) - bvq$ qui est une combinaison linéaire à coefficients entiers de a et b.

Si r n'était pas nul, on aurait trouvé un élément de E plus petit que d donc $r = 0$ donc $d|a$

On montrerait de même que $d|b$.

$d|a$ et $d|b$ donc $d|pgcd(a;b)$ donc $d \leq pgcd(a;b)$.

On a montré que $pgcd(a;b) \leq d$ et $d \leq pgcd(a;b)$ donc $d = pgcd(a;b)$ donc $ua + vb = pgcd(a;b)$. □

Remarque 5. ATTENTION Si $ua+vb = g$, g n'est pas forcément le $pgcd(a;b)$. Contre-exemple $1\times1+1\times1 = 2$ mais $2 \neq pgcd(1;1)$.

Remarque 6. Il n'y a pas unicité de u et v. Exemple $a = 18$ et $b = 30$. $pgcd(18;30) = 6 \begin{cases} 2 \times 18 + (-1) \times 30 = 6 \\ (-3) \times 18 + 2 \times 30 = 6 \end{cases}$

Exemple 5. Déterminer deux entiers relatifs u et v tels que $u \times 99 + v \times 75 = pgcd(99, 75)$

On détermine le $pgcd$ avec l'algorithme d'Euclide puis, en l'exploitant on exprime tous les restes en fonction de 99 et 75.

Théorème 12. ***Théorème de Bézout*** $\forall a, b \in \mathbb{N}^*$, $pgcd(a;b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}$, $ua + vb = 1$.

Démonstration. L'identité de Bézout justifie le sens direct. Montrons la réciproque. Supposons que $ua+vb = 1$. $pgcd(a;b)$ divise a et b donc divise $ua + vb$ donc divise 1. Donc $pgcd(a;b) = 1$. □

Remarque 7. Il n'y a pas unicité de u et v non plus. Exemple $a = 2$ et $b = 3$. $\begin{cases} (-1) \times 2 + 1 \times 3 = 1 \\ (-4) \times 2 + 3 \times 3 = 1 \end{cases}$.

Exemple 6. Soit $n \in \mathbb{N}$. Montrer que $2n + 1$ et $9n + 4$ sont premiers entre eux.

Exemple 7. Soit $n \in \mathbb{N}$. Déterminer $pgcd(2n + 1; 2n + 3)$.

2.2. **Travailler son cours.**

Exercice 3. Montrer que pgcd(5004 ;2002)=2 sans utiliser l'algorithme d'Euclide.

3. Théorème de Gauss

3.1. **Cours.**

Théorème 13. ***de Gauss*** *Soit* $a, b, c \in \mathbb{N}^*$. $\begin{cases} a|bc \\ pgcd(a;b) = 1 \end{cases} \Rightarrow a|c.$

Démonstration. $a|bc$ donc $\exists k \in \mathbb{N}$, $bc = ka$

$pgcd(a;b) = 1$ donc d'après le théorème de Bézout $\exists u, v \in \mathbb{Z}$, $ua + vb = 1$ donc $cau + cvb = c$ or $bc = ka$ donc $cau + kav = c$ donc $(uc + kv)a = c$ donc $a|c$. □

Corollaire 1. *Soit* $a, b, c \in \mathbb{N}^*$. $\begin{cases} a|c \\ b|c \\ pgcd(a;b) = 1 \end{cases} \Rightarrow ab|c.$

Démonstration. Supposons les hypothèses du théorème. $\exists k, k' \in \mathbb{N}$, $c = ka = k'b$ donc $a|k'b$ or $pgcd(a;b) = 1$ donc d'après le théorème de Gauss $a|k'$ donc $\exists k'' \in \mathbb{N}$, $k' = k''a$ or $c = k'b$ donc $c = k''ab$ donc $ab|c$. □

Exemple 8. Montrer que le produit de trois entiers naturels consécutifs est divisible par 6.

Exemple 9. Montrer que le produit de 4 entiers naturels consécutifs est divisible par 24.

Exemple 10. Arthur sait qu'il a entre 300 et 400 jetons. S'il fait des tas de 17 jetons, il lui en reste 9. S'il fait des tas de 5 jetons, il lui en reste 3. On cherche combien Arthur a de jetons.

1. Ecrire un algorithme permettant de déterminer tous les nombres de jetons possibles que possède Arthur. L'algorithme calculera le nombre de divisions euclidiennes qu'il effectue. Ne pas finasser, l'ordinateur est rapide !

La question posée se traduit par $\begin{cases} n \equiv 9\ [17] \\ n \equiv 3\ [5] \end{cases}$ (S)

2. a. Trouver des relatifs u et v tels que 17u+5v=1.

2.b. En déduire **une** solution n_0 de (S).

2.c. Quelle est la forme générale des solutions de (S) ?

3. Quel est le nombre de jetons d'Arthur

Exemple 11. Résoudre dans $\mathbb{Z}$ l'équation $22x + 138y = 102$ (E).

La calculatrice nous donne $pgcd(22; 138) =$. Cela permet de simplifier l'équation :

$(E) \Leftrightarrow$

Cherchons une solution particulière de cette équation :

Cette solution permet de supprimer le second membre de l'équation :

Supposons que $(x; y)$ est une solution de (E).

$\begin{cases} \quad \mid \quad (\quad) \\ pgcd(\quad ; \quad) = 1 \end{cases}$ donc d'après le théorème de Gauss $\mid$ donc $\exists k \in \mathbb{Z}$,

Exprimons x et y en fonction de k.

On a montré que si $(x;y)$ est solution de (E) alors $\exists k \in \mathbb{Z}$, $\left\{ \begin{array}{l} x = \\ y = \end{array} \right.$

Réciproquement, vérifions que tous les couples $(x;y)$ de cette forme sont solution de (E).

L'ensemble des solutions de (E) est

Chapitre C - Nombres premiers

1. Définition

1.1. Cours.

Définition 5. Un nombre naturel est **premier** s'il possède exactement deux diviseurs positifs : 1 et lui même.

Remarque 8. Est-ce que 0 est premier ? Est-ce que 1 est premier ?

2. Décomposition en produit de facteurs premiers

2.1. Cours.

Lemme 2. *Soit n un entier naturel non premier. Son plus petit diviseur différent de 1 est premier.*

Démonstration. Soit E l'ensemble des diviseurs de n privé de 1 et de lui-même. Comme n n'est pas premier, cet ensemble est non vide donc il admet un plus petit élément p.

Supposons que p n'est pas premier.

p possède donc un diviseur p' différent de 1 et de lui-même donc 1<p'<p

p'|p et p|n donc p'|n

p'|n et 1<p' donc p' est dans E or p'<p donc p n'est pas le plus petit élémént de E : CONTRADICTION !

On a montré par l'absurde que p est premier. □

Lemme 3. *Si p est premier avec a et avec b alors p est premier avec ab.*

Démonstration. Soit p premier avec a et b. D'après le théorème de Bézout il existe les relatifs u, v, u', v' tels que up+va=1 et u'p+v'b=1 donc 1=(up+va)(u'p+v'b)=(uu'p+uv'b+vu'a)p+vv'(ab) donc d'après le théorème de Bézout p est premier avec ab. □

Remarque 9. Ce lemme se généralise par récurrence à un nombre quelconque de facteurs.

Théorème 14. *Tout entier naturel supérieur ou égal à 2 se décompose en produit de facteurs premiers. Cette décomposition est unique à l'ordre près des facteurs. On note alors :* $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ *où* p_1, p_2, ..., p_r *sont des nombres premiers distincts et* α_1, α_2, ..., α_r *sont des entiers naturels non nuls.*

Démonstration.

Existence

Si n est premier : la propriété est établie.

Sinon :

Soit p_1 le plus petit diviseur de n différent de 1. Ce nombre existe et est premier d'après le premier lemme. Soit $n_1 = \frac{n}{p_1}$. $n_1 < n$

Si n_1 est premier : la propriété est établie.

Sinon : on répète le processus en définissant p_2, n_2 etc

On crée ainsi une suite d'entiers n_i naturels strictement décroissante. Cette suite est nécessairement finie et son dernier terme est premier.

En regroupant les facteurs, on obtient : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$.

Unicité

Soit P_n : "La décomposition est unique pour tout entier naturel inférieur ou égal à n".

Initialisation

P_2 est évident.

Hérédité

Soit $n-1$ un entier tel que P_{n-1}.

Supposons que n admette deux décompositions distinctes en produit de facteurs premiers.

$n = p_1 \times p_2 \times ... \times p_r = q_1 \times q_2 \times ... \times q_s$

Si p_1 était premier avec tous les q_i, alors d'après le deuxième lemme, p_1 serait premier avec $q_1 \times q_2 \times ... \times q_s$, mais c'est impossible car p_1 divise $q_1 \times q_2 \times ... \times q_s$. On a donc montré par l'absurde qu'il existe un i tel que p_1 n'est pas premier avec q_i. Comme ce sont des nombres premiers, on a nécessairement $p_1 = q_i$ or les décompositions de départ étaient distinctes donc les deux décompositions suivantes sont distinstes :

$p_2 \times ... \times p_r = q_1 \times ... \times q_{i-1} \times q_{i+1} \times ... \times q_s$

ce qui contredit l'hypothèse de récurrence.

On a montré P_n par l'absurde.

Conclusion

On a montré par récurrence que la décomposition en facteurs premiers est unique. □

Exemple 12. En utilisant la décomposition en facteurs premiers, déterminer le pgcd et le ppcm de 13734 et 91260.

Lemme 4. *Soit p un nombre premier et a et b deux entiers naturels. Si $p|ab$ alors $p|a$ ou $p|b$.*

Démonstration. □

Remarque 10. Ce lemme se généralise par récurrence à un nombre quelconque de facteurs.

Théorème 15. *Soit $p_1^{\alpha_1} \times ... \times p_r^{\alpha_r}$ la décomposition d'un entier naturel n en facteurs premiers. Les diviseurs d de n sont de la forme $d = p_1^{\beta_1} \times ... \times p_r^{\beta_r}$ où les β_i vérifient $0 \leq \beta_i \leq \alpha_i$.*

Démonstration. Les nombres de la forme de la forme $p_1^{\beta_1} \times ... \times p_r^{\beta_r}$ où les β_i vérifient $0 \leq \beta_i \leq \alpha_i$ sont clairement des diviseurs de n.

Réciproquement, soit d un diviseur de n. Tout facteur premier de d divise n donc d'après le lemme, divise l'un des p_i donc est égal à p_i. On en déduit en regroupant les facteurs que d peut s'écrire sous la forme $d = p_1^{\beta_1} \times ... \times p_r^{\beta_r}$.

Il reste à montrer que pour tous les i, $0 \leq \beta_i \leq \alpha_i$. Si ce n'était pas le cas pour un i donné, on en déduirait que p_i divise un nombre dont la décomposition en facteurs premiers ne contient pas p_i ce qui est impossible d'après ce qu'on vient de montrer. □

Exemple 13. Déterminer le nombre de diviseurs de 13000.

Chapitre D - Matrices et évolution de processus

1. Matrices

1.1. Cours.

Définition 6. Soit p et q deux entiers naturels non nuls. On appelle **matrice** à p lignes et q colonnes un tableau de nombres réels à p lignes et q colonnes. Pour la matrice A, ces nombres, appelés coeficients de la matrice, sont notés a_{ij} où i est le numéro de la ligne et j celui de la colonne.

$$A = \begin{pmatrix} a_{11} & \dots & a_{1q} \\ \dots & & \dots \\ a_{p1} & \dots & a_{pq} \end{pmatrix}$$

Remarque 11. Si p=q on parle de matrice carrée. Si p=1 on parle de matrice ligne. Si q=1 on parle de matrice colonne.

Exemple 14. Les coordonnées des points sont des matrices ligne. Les coordonnées des vecteurs sont des matrices colonnes.

Théorème 16. *Deux matrices sont égales ssi elles ont les mêmes dimensions et leurs coefficients sont égaux.*

Définition 7. Si A et B sont deux matrices $p \times q$, on définit la matrice $C = A + B$ comme la matrice $p \times q$ telle que pour tout entier i entre 1 et p et tout entier j entre 1 et q, $c_{ij} = a_{ij} + b_{ij}$.

Définition 8. Si A est une matrice $p \times q$ et λ un réel, on définit la matrice $C = \lambda A$ comme la matrice $p \times q$ telle que pour tout entier i entre 1 et p et tout entier j entre 1 et q, $c_{ij} = \lambda a_{ij}$.

Définition 9. Si A est une matrice $p \times q$ et B une matrice $q \times r$, on définit la matrice $C = A \times B$ comme la matrice $p \times r$ telle que pour tout entier i entre 1 et p et tout entier k entre 1 et r, $c_{ik} = \sum_{j=1}^{q} a_{ij} b_{jk}$.

Remarque 12. Les seuls cas véritablement au programme sont :

- p=q=r
- p=q et r=1
- p=1 et q=r

Exemple 15. p=q=r=3

$$\begin{pmatrix} 1 & 0 & 2 \\ -1 & -1,5 & 0 \\ 4 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 3 \\ 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

Exemple 16. p=q=3 r=1

$$\begin{pmatrix} 1 & 0 & 2 \\ -1 & -1,5 & 0 \\ 4 & 0 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} \\ \\ \end{pmatrix}$$

Exemple 17. p=1 q=r=3

$$\begin{pmatrix} 3 & 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \\ -1 & -1,5 & 0 \\ 4 & 0 & 0 \end{pmatrix} = \begin{pmatrix} & & \end{pmatrix}$$

Théorème 17. *Soit A, B, C des matrices carrées de même taille. Soit k et k' des réels.*

(1) $A + B = B + A$

(2) $(A+B)+C = A+(B+C)$

(3) $(k+k')A = kA+k'A$

(4) $k(A+B) = kA+kB$

(5) $(kk')A = k(k'A)$

(6) $(kA)B = A(kB) = k(A\times B)$

(7) $(A\times B)\times C = A\times(B\times C)$

(8) $A\times(B+C) = A\times B + A\times C$

(9) $(A+B)\times C = A\times C + B\times C$

Remarque 13. En général $A\times B \neq B\times A$.

Notation 3. $A\times A = A^2$ $A\times A\times A = A^3$ etc

Exemple 18. Utilisation de la calculatrice (noter ici votre mode d'emploi)

$$A = \begin{pmatrix} 1 & -3 & 2 \\ 4 & 7,5 & 0 \\ 6 & 5 & -1 \end{pmatrix} \quad B = \begin{pmatrix} \frac{1}{3} & \frac{2}{7} & \frac{1}{4} \\ 4 & \frac{10}{11} & 0 \\ 6 & 5 & -\frac{1}{2} \end{pmatrix}$$

$$A+\tfrac{2}{3}B = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \quad A\times B = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

On crée d'abord les matrices en entrant leurs coefficients (TI : mode matrice, mode EDIT, nb de lignes, nb de colonnes), (CASIO : RUNMAT, mode matrice F3 -> MAT, nb de lignes, nb de colonnes). On effectue les calculs en rappelant les matrices par leur nom (TI : sélectionner leur nom dans le mode matrice, pour les coefficients frationnaires MATH mode FRAC), (CASIO : précéder leur nom de MAT, pour les coefficients fractionnaires F<->D).

2. Evolution de processus

2.1. Cours.

Définition 10. Si les **états possibles d'un processus** sont numérotés de 1 à n on peut les représenter par une matrice ligne ou une matrice colonne de dimension n. Le kième coefficient représente la proportion d'individus dans l'état k ou la probabilité qu'un individu soit dans l'état k.

Définition 11. On appelle **matrice de transition** une matrice carrée $n\times n$ définie ainsi. Le coefficient à la ligne i et la colonne j donne

- la probabilité de transition de l'état i à l'état j dans le cas d'états modelisés par une matrice ligne,
- la probabilité de transition de l'état j à l'état i dans le cas d'états modelisés par une matrice colonne.

Remarque 14. Si les états sont modelisés par une matrice ligne, la somme des coefficients d'une ligne de la matrice de transition vaut 1. Si les états sont modelisés par une matrice colonne, la somme des coefficients d'une colonne de la matrice de transition vaut 1.

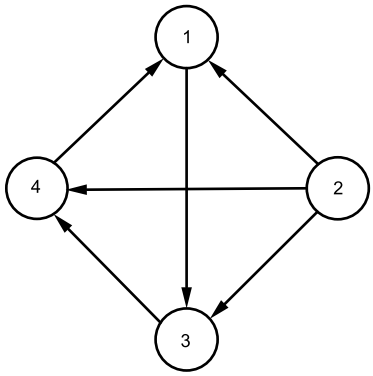
Définition 12. Lorsqu'il s'agit de probabilités, on parle de **marche aléatoire**. Dans ce cas, la matrice de l'état après n transitions est appelée **état de la marche aléatoire après n pas.**

Théorème 18. *Soit une marche aléatoire de matrice de transition A et de matrice de l'état après n pas X_n.*

- $\forall n\in\mathbb{N}$, $X_{n+1} = X_nA$ et $X_n = X_0A^n$ dans le cas d'états modelisés par une matrice ligne,
- $\forall n\in\mathbb{N}$, $X_{n+1} = AX_n$ et $X_n = A^nX_0$ dans le cas d'états modelisés par une matrice colonne.

2.2. **Travailler son cours.**

Exercice 4. Ecrire la matrice de transition associée au graphe ci-contre. A chaque pas on passe d'un sommet à un autre par une arête issue de ce sommet choisie de façon équiprobable. Les états sont représentés par des matrices colonnes.



Chapitre E - Matrices carrées inversibles

1. Matrice inverse

1.1. Cours.

Définition 13. On appelle **matrice unité de taille (ou d'ordre) n**, la matrice I_n dont tous les coefficients sont nuls exceptés ceux de la diagonale issue du coin en haut à gauche qui valent tous 1.

Théorème 19. *Pour toute matrice carrée A de taille n,* $A \times I_n = I_n \times A = A$.

Remarque 15. Par convention, pour toute matrice carrée A de taille n, $A^0 = I_n$.

Définition 14. Soit A une matrice carrée de taille n. A est inversible s'il existe une matrice B telle que $A \times B = B \times A = I_n$. On dit alors que B est l'inverse de A et on note $B = A^{-1}$.

Théorème 20. *Pour montrer que A est inversible il suffit de montrer que* $A \times B = I_n$ *ou* $B \times A = I_n$.

Démonstration. On admet ce théorème. □

Théorème 21. *Soit A une matrice inversible de taille n.*

Pour toutes matrices M et N carrées ou lignes de taille n : $M \times A = N \Leftrightarrow M = N \times A^{-1}$

Pour toutes matrices M et N carrées ou colonnes de taille n : $A \times M = N \Leftrightarrow M = A^{-1} \times N$.

Démonstration. □

Exemple 19. Soit $M = \begin{pmatrix} 3 & 3 \\ 4 & 6 \end{pmatrix}$ et $N = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Résoudre $MX = X + N$.

Théorème 22. *Soit A une matrice inversible. Pour tout réel* $k \neq 0$*, la matrice kA est inversible et sa matrice inverse est* $\frac{1}{k}A^{-1}$.

Démonstration. □

Remarque 16. Vérifier que vous savez déterminer l'inverse d'une matrice avec votre calculatrice. Si $A = \begin{pmatrix} 10 & -2 \\ -18 & 4 \end{pmatrix}$ alors vous devez trouver $A^{-1} = \begin{pmatrix} 1 & 0,5 \\ 4,5 & 2,5 \end{pmatrix}$.

Théorème 23. *Soit* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *M est inversible ssi* $ad - bc \neq 0$.

Démonstration. Voir l'Activité. □

1.2. **Travailler son cours.**

Exercice 5. Soit A et B des matrices inversibles. Quelle est l'inverse de $A \times B$?

2. Applications

2.1. **Cours.**

Théorème 24. *Soit AU=V l'écriture matricielle d'un système linéaire.*

- Si la matrice A est inversible, le système a une unique solution égale à $A^{-1}V$.
- Sinon le système a soit une infinité de solutions soit pas de solution.

Démonstration. Voir l'Activité pour la justification du deuxième point. □

Exemple 20. Soit A(1 ;-2 ;4) B(-2 ;-6 ;5) C(-4 ;0 ;-3). Montrer que ces 3 points définissent un plan et déterminer une équation de ce plan.

Exemple 21. Soit $A = \begin{pmatrix} 6,25 & -9 \\ 4,5 & -6,5 \end{pmatrix}$ $D = \begin{pmatrix} 0,25 & 0 \\ 0 & -0,5 \end{pmatrix}$ $P = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$. Vérifier que $A = P \times D \times P^{-1}$. En déduire l'expression de A^n.

Chapitre F - Matrices et études asymptotiques

1. Suites récurrentes et matrices

1.1. Cours.

Exemple 22. Soit deux suites définies par $\begin{cases} u_0 = 5 \\ v_0 = -2 \\ \forall n \geq 0,\ u_{n+1} = 1,7u_n + 0,6v_n + 3 \\ \forall n \geq 0,\ v_{n+1} = -5u_n + 0,1v_n - 1 \end{cases}$. Calculer les termes successifs de ces suites à l'aide du calcul matriciel.

Exemple 23. Soit une suite définie par $\begin{cases} u_0 = 11 \\ u_1 = -2 \\ \forall n \geq 0,\ u_{n+2} = 3u_{n+1} - 0,5u_n \end{cases}$. Calculer les termes successifs de cette suite à l'aide du calcul matriciel.

Théorème 25. *Soit une suite de matrices colonnes (X_n) telle que pour tout entier $n \geq 0$, $X_{n+1} = AX_n$. Alors pour tout $n \geq 0$ $X_n = A^n X_0$.*

Démonstration. Par récurrence. □

Remarque 17. Il y a un théorème analogue avec des matrices lignes.

2. Convergence et etat stable

2.1. Cours.

Remarque 18. Tout ce qui est dit jusqu'à la fin de ce chapitre peut être transposé au cas des matrices lignes ;

Définition 15. On dit que la **suite de matrices** colonnes (X_n) de taille p est **convergente** ssi les suites formées par les coefficients sont convergentes. La limite de cette suite est alors la matrice colonne formée par les p limites obtenues.

Dans tous les autres cas, on dit que la suite est **divergente**.

Théorème 26. *Si une suite de matrices colonnes (X_n) vérifiant une relation de récurrence du type $X_{n+1} = AX_n + B$ est convergente, alors sa limite X vérifie $X = AX + B$.*

Démonstration. □

Remarque 19. Si une suite est définie par une relation de récurrence de ce type et si l'équation X=AX+B a une solution, la suite n'est pas forcément convergente. Contre-exemple : $X_0 = \begin{pmatrix}1\\1\end{pmatrix}$ $A = \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ $B = \begin{pmatrix}0\\0\end{pmatrix}$.

Remarque 20. Si l'équation $X = AX + B$ n'a pas de solution, la suite (X_n) ne peut pas converger.

Remarque 21. Si l'équation $X = AX + B$ a une infinité de solutions, d'autres conditions liées à la limite permettent parfois de restreindre les limites **envisageables**.

3. Application aux marches aléatoires

3.1. Cours.

Définition 16. On dit qu'une **marche aléatoire** est **convergente** si la suite des états est convergente.

Définition 17. Si la suite des états vérifie une relation du type $X_{n+1} = AX_n + B$, une suite constante vérifiant $X = AX + B$ est appelée **état stable** de la marche aléatoire.

Remarque 22. Une marche aléatoire peut être convergente ou divergente selon l'état initial X_0. S'il y a convergence, ce ne peut être que vers un état stable.

Exemple 24. Etudier la convergence de la marche aléatoire définie par $A = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ $B = \begin{pmatrix}0\\0\end{pmatrix}$ $X_0 = \begin{pmatrix}a\\b\end{pmatrix}$.

Théorème 27. *Soit $p, q \in]0;1[$. Soit la marche aléatoire de matrice de transition $M = \begin{pmatrix}1-p & q\\p & 1-q\end{pmatrix}$. Quel que soit l'état initial X_0 de cette marche aléatoire, elle converge vers un état stable unique $X = \begin{pmatrix}a\\b\end{pmatrix}$ tel que $X = MX$ et $a + b = 1$.*

Démonstration. comportant des questions ne participant pas directement à la démonstration mais intéressantes ... □

Commencer par donner le graphe probabiliste associé.

Soit $X_n = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$. Pourquoi a-t-on $a_n + b_n = 1$?

Déterminer tous les états stables $X = \begin{pmatrix} a \\ b \end{pmatrix}$.

Comment peut-on restreindre les limites envisageables ? Le faire.

Déterminer une relation entre a_{n+1} et a_n.

Soit la suite définie par $u_n = a_n - \frac{q}{p+q}$. Montrer que cette suite est une suite géométrique qui converge vers 0.

En déduire que (a_n) et (b_n) sont convergentes et déterminer leurs limites. Vérifier que ces limites ne dépendent pas de X_0.